UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v.-

KUN SHAN CHUN,
a/k/a "Joey Chun,"

Defendant.

16 Cr. 518 (VM)

GOVERNMENT'S SENTENCING MEMORANDUM

PREET BHARARA,
United States Attorney for the
Southern District of New York,
Attorney for the United States
of America.

Emil J. Bove III,
Assistant United States Attorney
Of Counsel.

TABLE OF CONTENTS

Page

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA -v.- KUN SHAN CHUN, a/k/a "Joey Chun," Defendant.	16 Cr. 518 (VM)

The Government respectfully submits this memorandum in connection with the sentencing of the defendant, Kun Shan Chun, a/k/a "Joey Chun," which is scheduled for January 20, 2017 at 3:00 p.m. For the reasons set forth below, the Government respectfully submits that a sentence of 27 months' imprisonment is appropriate and that a fine of $95,000 should be imposed.

BACKGROUND

The defendant acted as an agent of the People's Republic of China, while he worked at the Federal Bureau of Investigation ("FBI") in New York, in violation of Title 18, United States Code, Section 951(a). For almost 20 years, the FBI employed the defendant as an electronics technician and entrusted him with sensitive information requiring a Top Secret security clearance. But the defendant engaged in a prolonged deception of the FBI and the United States—lasting for nearly a decade—by maintaining undisclosed relationships with Chinese nationals, which he developed during paid-for trips abroad while they cultivated him as a source of information, and later acting at the direction of an official of the Chinese government ("Chinese Official-1") to gather and send sensitive FBI information to China.

In response to taskings from Chinese Official-1, the defendant is known to have taken the following steps:

- During a trip to Europe in 2011, the defendant disclosed to Chinese Official-1 the name of an FBI Special Agent, the Agent's duties at the FBI, and a location in Asia where the Agent traveled because he had relatives there.

- In March 2013, the defendant downloaded from his FBI computer an organizational chart relating to the FBI's New York Special Operations Group. The defendant provided the document on a piece of storage media to a member of his immediate family ("Relative-1") so that she could deliver it to Chinese Official-1 in China.

- In January 2015, the defendant used his FBI-issued phone to take a series of photographs of fliers at the FBI, which were posted in a restricted space in an FBI office, relating to sensitive technologies used by the FBI. The defendant sent the photographs to his personal phone, and then provided them to Relative-1 so that she could deliver them to Chinese Official-1 in China.

- During the course of the defendant's interactions with Chinese Official-1, he also disclosed, at minimum, general information regarding the FBI's surveillance strategies and certain categories of surveillance targets.

After taking these actions, beginning in approximately February 2015, the defendant admitted to an FBI undercover employee (the "UC") that he had intentionally concealed his relationships with Chinese Official-1 and other Chinese nationals, and discussed with the UC a plan to provide so-called "consulting" services to Chinese nationals in exchange for pay, including the sale of sensitive information. In July 2015, the defendant started to speak with the UC about selling the Chinese government classified information, which the UC said that he could obtain from a United States government agency. About a month later, during a clandestine meeting in a hotel room in Manhattan, the defendant reviewed a classified document provided by the UC. The defendant expressed hesitation about the transaction, explaining to the UC that his reaction was based in part on concerns that he was already being investigated and that his Chinese associates had advised him to be wary of the UC. In October 2015, however, the defendant asked the UC to maintain possession of the classified document until "the time is right," which the defendant said

would allow him to have a "clean mind" during an anticipated FBI polygraph in 2016, "beat the . . . system" during the related routine examination of his security clearance, and have "time to play"—likely by facilitating the sale of the classified document—after his security clearance was renewed.

Put simply, this offense merits substantial punishment. The defendant's conduct was egregious, and the harm he is known to have caused significant. Moreover, in the face of escalating threats posed by foreign intelligence actors to the security of sensitive and classified information in the United States, including through the recruitment of United States personnel by foreign governments, general deterrence is a critical feature of this sentencing.[1] Therefore, the Government respectfully submits that a term of imprisonment of 27 months and a $95,000 fine—both at the top of the stipulated ranges in the parties' plea agreement—are appropriate.

A. The Defendant's Employment at the FBI

The defendant is a naturalized citizen who was born in Guangdong, China, in 1969. (Oct. 21, 2016 Presentence Investigation Report ("PSR") ¶ 39). He entered the United States in 1980, and became a naturalized citizen of the United States in 1985. (*Id.* ¶ 43). He earned a bachelor's degree in Electrical Engineering at a college in the United States. (*Id.* ¶ 54).

Between 1997 and 2016, the defendant worked as an electronics technician in the FBI's New York Field Office. (*Id.* ¶ 7).[2] In order to participate in these employment activities, the

[1] "The United States faces a large and growing threat to its national security from Chinese intelligence collection operations. Among the most serious threats are China's efforts at cyber and human infiltration of U.S. national security organizations. These operations are not a recent phenomenon, but reports of Chinese espionage against the United States have risen significantly over the past 15 years." U.S.-China Econ. and Sec. Review Comm'n, *2016 Report to Congress*, ch. 2, § 3 at 289 (the "2016 U.S.-China Report") (Nov. 16, 2016), *attached as* Exhibit A and *available at* http://www.uscc.gov/Annual_Reports/2016-annual-report-congress (last accessed Jan. 6, 2017).

[2] The defendant was suspended by the FBI around the time of his arrest in May 2016 pending the

defendant was granted a Top Secret security clearance in 1998. (*Id.* ¶ 8). At the time of the defendant's arrest, he earned approximately $97,000 per year. While employed at the FBI, the defendant was placed in a unit responsible for technical tasks related to the implementation and maintenance of court-ordered electronic surveillance (including pursuant to the Foreign Intelligence Surveillance Act), he worked on FBI network infrastructure inside and outside Sensitive Compartmented Information Facilities (known as SCIFs), and he helped install and upgrade hardware and software at multiple FBI facilities in New York and New Jersey.

B. The Initial Recruitment of the Defendant

Beginning in approximately 2005, the foundation for the defendant's activities on behalf of the Chinese government was laid through financial benefits provided to the defendant and his relatives via purported managers of an entity named Zhuhai Kolion Technology Company Ltd. ("Kolion"). (PSR ¶ 10). According to a publicly available website, Kolion is a China-based manufacturer of printer products.[3]

The defendant's illicit relationships appear to have been initiated when Chinese individuals purporting to be affiliated with Kolion solicited an investment from Relative-1.[4] The defendant then had direct contact with purported associates of Kolion during a December 2005 trip

---

conclusion of an administrative termination procedure (PSR ¶ 56), and his termination became final on January 5, 2017.

[3] *See* KolionTech, http://www.koliontech.com (last accessed January 6, 2017). In May 2016, a trade publication titled the *Recycling Times* posted a statement from Mito Color Imaging Co., Ltd. ("Mito"), which indicated that Mito had acquired Kolion in approximately 2014, and that neither the defendant nor his relatives had ever been associated with Kolion. *See* Mito Response to False Rumors, *Recycling Times*, http://www.irecyclingtimes.com/News-Detail?news_column_id=16&news_id=6956 (last accessed January 7, 2017).

[4] As used in this submission, references to "Chinese nationals," the defendant's "Chinese associates," and the defendant's "Chinese contacts" are intended to mean Chinese nationals purporting to be affiliated with either Kolion, Chinese Official-1, or both, and to exclude, for example, other relatives of the defendant in China.

with Relative-1 to Hong Kong and Guangdong, China, which he reported to the FBI at the time as merely a vacation. Following the trip, in January 2006, the defendant sent an email to one of the Chinese nationals purportedly affiliated with Kolion ("CC-1"), which stated in part:

> Just want to take [] this opportunity to thank you for a very informative [] introduction to your company, and [I] have learned a lot about your operation. I am very delighted that [I] met you and [another purported Kolion employee ("CC-2")]. I hope we will continue to work together in the future. Below is my Skype User Name and emails. Please relate this email to [CC-2] too."

The defendant included in the email a Skype account, three email addresses, a telephone number, and his physical address, and he asked that they "start communicating soon through the internet."

C. The Defendant's Recruitment By Chinese Nationals and Chinese Official-1

Between the defendant's late-2005 meeting in China and the FBI's 2012 routine reinvestigation of his security clearance, he left the United States at least six times to either meet with purported Kolion personnel or take trips that were funded in whole or in part by these individuals.

1. 2007: Singapore, Malaysia, and China

On November 27, 2007, the defendant sent an email to CC-2 that contained passport numbers for the defendant and Relative-1, among others. On November 30, 2007, the defendant departed on a trip that he initially told the FBI would include stops in Hong Kong and mainland China, but which he later disclosed to the FBI also included stops in Singapore and Malaysia. During the trip, the defendant met with CC-1 and CC-2, and CC-2 told the defendant that one of his relatives—Chinese Official-1—worked for the Chinese government. The defendant did not disclose anything about these foreign contacts to the FBI, despite being required to do so, until after he was arrested in 2016.

After the defendant returned from China, on December 18, 2007, CC-1 sent the defendant an email indicating that he had learned a lot from their discussions and asking the

defendant to review an attachment relating to a printer cartridge. The defendant forwarded the email to another member of his immediate family ("Relative-2"). On February 27, 2008, the defendant sent another message to Relative-2, which suggested he had further contact with purported employees of Kolion regarding the tasking and compensation:

> Actually those guys want[] us to help them out to buy the device do[] all the programming, and erase them entirely . . . . According to them, they will give us money for the time we spend[] on this research, and they will pay us back if they decided [to] let us . . . buy the[] equipment[].

2. 2009: China

On May 20, 2009, the defendant received an email addressed to shareholders of Kolion and signed by CC-2. Weeks later, CC-2 sent an email to the defendant regarding Kolion's five-year anniversary. The defendant responded: "[M]e and [Relative-1] congratulate you and your company's successful[] years. . . . Hopefully in the future I will have time to visit you and your company."

On November 9, 2009, the defendant sent CC-2 passport numbers for himself and other relatives. On December 6, 2009, the defendant left the United States on a trip that he reported to the FBI would include stops in Hong Kong and Guangdong. During the trip, however, CC-1 and CC-2 paid for the defendant to travel with them to Thailand. When the defendant returned, he wrote to Relative-2 on January 7, 2010, among other things:

> [I] need to get SSD [solid-state hard drive] for the people in China . . . they are paying . . . [I] want to order them and have [a relative] bring them back to them, because she is leaving on the 13 . . . . they want to wire money to me, but [I] told them [I] pay for it now, and just give money to [a relative] so he can bring it back.

3. 2010: Saipan and China

In May 2010, the defendant traveled to Saipan to meet with CC-1 and at least one other purported Kolion employee ("CC-3"). CC-1 or other purported Kolion employees paid for the defendant's lodging and meals during the trip, as well as a day-trip to a nearby island via

private plane. The defendant admitted to the FBI following his arrest that his Chinese associates brought several women to one or more of their meetings, and that he had a romantic relationship with one of the women that continued until at least approximately 2012. During an August 2015 meeting with the UC, the defendant indicated that Saipan's status as a commonwealth of the United States meant that he did not have to report travel there to the FBI or pass through U.S. customs if he was carrying cash.

On October 14, 2010, the defendant wrote to Relative-2: "[Y]ou know where I can go to find companies that do remanufacturing toner cartridges[?] . . . [T]he company in china needs that information quick[.]" After Relative-2 sent the defendant a link to a website, he responded: "[I] need a lot more[.] [S]o I can give them a report. . . . [I] think they need some market research so that if they get [sued] by [a] brand name company in the future, they can use these data to fight back." Less than two months after these emails, the defendant traveled to China on a trip that he told the FBI was for "sight-seeing" with members of his immediate family.

4. 2011: Europe

On September 29, 2011, CC-2 sent an email to the defendant that included information relating to hotels in France and Italy and stated "Five Star Hotel the entire way." The defendant responded by sending full names and passport numbers for himself and another relative ("Relative-3"). The following day, the defendant forwarded some of the hotel information from CC-2 to Relative-2 and another relative with a message that stated: "It's a short notice, [I] got invited to a 10 day[] trip to Europe by the company in China. . . . [Relative-3] is travel[]ing with me, well her ticket has to pay for."

On October 5, 2011, the defendant and Relative-3 departed on a trip to France and Italy. The defendant's Chinese associates paid for their hotels and expenses. At least once during the trip, the defendant met privately with Chinese Official-1 in a hotel room. (PSR ¶ 12). Chinese

Official-1 confirmed that he worked for the Chinese government, and that he knew the defendant worked for the FBI. During the meeting, the defendant disclosed to Chinese Official-1 the name of an FBI Special Agent, the agent's duties at the FBI, and that the Agent sometimes traveled to a location in Asia because he has relatives there. Over the course of their relationship, Chinese Official-1 asked the defendant questions regarding the FBI's personnel, structure, technological capabilities, surveillance practices, and Chinese surveillance targets. (*Id.* ¶ 12).

D. The Defendant's False Statements to the FBI

During the same timeframe that the defendant formed relationships with CC-1, CC-2, CC-3, and ultimately Chinese Official-1, the FBI emphasized during training provided to its employees—including the defendant—the importance of reporting contacts with foreign nationals and agents of foreign powers, and the risks associated with foreign travel. For example, in 2007, the FBI provided the defendant with a briefing document summarizing the risk that he could be targeted by a foreign intelligence agency, including through "Recruitment," *i.e.*, "The attempt to establish a clandestine relationship with a subject through his/her voluntary cooperation." In November 2009, the defendant signed a document confirming that he had received a "Foreign Travel/Hit Briefing," which included warnings of this nature:

- "Foreign intelligence services are interested in you because you are an American, you are a U.S. Government employee, you work in the Intelligence Community, you have access to sensitive information & you work in Law Enforcement."

- "Typical approaches [by Foreign intelligence services] include: Recruitment: The attempt to establish a clandestine relationship with a subject through his/her voluntary cooperation."

In an effort to avoid breaches like the defendant's, the FBI takes steps to monitor foreign travel by its employees. These efforts include a requirement that FBI employees must provide information regarding their travel prior to taking an international trip, including the

purpose of the trip, the planned itinerary, anticipated travel companions, and anticipated contact with foreign nationals. FBI employees are also required to participate in debriefings upon returning from an international trip, which often include a written questionnaire as well as an interview. Although the defendant completed the FBI's required travel forms in connection with foreign travel that continued until the summer of 2015, many of his submissions contained glaring omissions—and in some instances outright lies—relating to his contact and ongoing relationships with Chinese Official-1 and other Chinese nationals.

The FBI conducts routine background checks on employees granted security clearances. The FBI conducted such investigations of the defendant in or about 2002, 2007, and 2012, and he was to undergo another one in 2016. Due to the defendant's contact with purported Kolion personnel beginning in late 2005, the information that he provided in connection with the FBI's 2007 investigation was, at best, highly misleading. The defendant told the FBI that he had "never been approached by anyone trying to convince him to work for a foreign government or company," and "never been approached by anyone in what he believed was an attempt to recruit him to work for a foreign government or company." In light of what had transpired by the end of 2011, including most notably the defendant's disclosures of sensitive FBI information to Chinese Official-1, his conduct during the 2012 reinvestigation was criminal. (PSR ¶ 13). In February 2012, the defendant completed an "Electronic Questionnaire for Investigations Processing," which he acknowledged was being submitted subject to criminal penalties for false statements pursuant to Title 18, United States Code, Section 1001. The defendant falsely answered "No" to the following questions:

- "Do you have, or have you had, close and/or continuing contact with a foreign national within the last seven (7) years with whom you, or your spouse, or cohabitant are bound by affection, influence, common interests, and/or obligation?"[5]

- "Have you in the past seven (7) years provided advice or support to any individual associated with a foreign business or other foreign organization that you have not previously listed as a former employer?"

- "Have you in the past seven (7) years been involved in any other type of business venture with a foreign national not described above (own, co-own, serve as a business consultant, provide financial support, etc.)?"

In 2007 and 2012, the defendant's routine background checks included polygraph examinations, during which the defendant concealed relationships with, and financial benefits received from, Chinese Official-1 and other Chinese nationals.

E. The Defendant's Disclosure of Additional Sensitive FBI Information to the Chinese Government

With his security clearance having survived the FBI's 2012 routine background investigation, the defendant continued his undisclosed contacts with Chinese nationals, including Chinese Official-1, and provided additional sensitive FBI information to them.

1. The Defendant Steals and Sends to Chinese Official-1 an FBI Organizational Chart in Exchange for a Mediterranean Cruise

On March 4, 2013, the defendant downloaded from his FBI computer an organizational chart relating to the FBI's New York Special Operations Group. He provided the document on a piece of storage media to Relative-1 so that she could deliver it to Chinese Official-1. (PSR ¶¶ 8(b), 14).[6] Relative-1 flew to Hong Kong on March 5, 2013. In December 2013, the

[5] The questionnaire defined the term "foreign national" as "any person who is not a citizen or national of the U.S."

[6] Although the defendant's post-arrest description of this conduct evolved over time, he asserted that he edited the chart to remove the names of FBI personnel and retain only their titles. (*See* PSR ¶ 14). The FBI later identified some electronic evidence that tends to corroborate this claim.

defendant's Chinese associates paid, at least partially, for him and Relative-3 to take a cruise in the Mediterranean, including stops in Italy, France, Spain, and Tunisia.

2. The Defendant Steals and Sends to Chinese Official-1 Information Regarding FBI Electronic Surveillance in Exchange for a European Vacation

In September 2014, the defendant and Relative-3 met purported Kolion personnel and Chinese Official-1 for several weeks in Australia and New Zealand. On January 14, 2015, the defendant used his FBI-issued phone to take a series of photographs of fliers at the FBI—which were posted in restricted space in an FBI office—relating to sensitive electronic surveillance technologies used by the FBI. (PSR ¶¶ 8(c), 15). The defendant sent the photographs to his personal phone, and then provided them to Relative-1 to deliver to Chinese Official-1 in China. (*Id.*). Relative-1 flew to Hong Kong on January 15, 2015. As discussed in more detail below, during the summer of 2015, the defendant traveled to several countries in Europe in connection with a trip that was partially paid for by his Chinese associates.

F. The Defendant's Negotiations Relating to the Sale of Classified Information

In approximately February 2015, the FBI caused the UC to be introduced to the defendant. The UC purported to be working with another government agency. (PSR ¶ 16).

In March 2015, the defendant told the UC that Chinese nationals had previously asked him to "consult" by providing "ideas" relating to "technology," and to ship materials from the United States to them in China. (PSR ¶ 17).[7] Later in the meeting, the defendant indicated that his Chinese associates "deal with the [Chinese] government" and "probably have some government people." (*Id.*). The defendant also admitted that his Chinese associates sometimes paid for prostitutes for him when they met abroad, that Relative-1 owned an equity stake in

[7] Except where otherwise noted, quotations and summaries from meetings between the defendant and the UC, in both this submission and the PSR, are based on transcriptions of the recordings of the meetings that were prepared by the FBI.

Kolion, and that certain members of his immediate family (including Relative-1) had been paid by his Chinese associates. (*Id.*).

During a subsequent meeting in March 2015, the defendant reiterated that Kolion had "government backing," and that Relative-1 met a "section chief" about five years' prior whom the defendant believed worked for the Chinese government. (*Id.*). The defendant told the UC: "I know this [Chinese] government guy . . . if you deal with the government, you know what they want," "[t]hey want what the American government is doing . . . . Either trying to copy it or . . . information they want to know."

In April 2015, the defendant told the UC that his Chinese associates had asked him to "[l]ook for some talented people for us," and that they had proposed that the defendant travel to Europe for a meeting that summer. The defendant said that he thought the UC was a "very good candidate for this type of work," and that the defendant's Chinese contacts would probably pay for the UC to travel to a meeting with them in either Europe or China. The defendant also indicated that if the UC ever got "work in China" that he would be paid in cash. The following day, the defendant told the UC that he avoided communicating with his Chinese associates by phone "if it's anything important" because his phones could be wiretapped, adding that there was a "big possibility" his "work phone" was "monitored" and a chance that his personal phone was subject to surveillance as well.

Following the April 2015 meetings, the defendant expressed concern to the UC that he and Relative-3 were being investigated by law enforcement. He nevertheless met again with the UC in late-June 2015. During that meeting, the defendant and the UC agreed to meet in Europe in early July so that the defendant could introduce the UC to his Chinese associates. The defendant told the UC that he informed his associates that the UC was a consultant who may be in

a position to assist them. The defendant also said during the meeting that he wished to act as a "sub-consultant" to the UC and wanted the UC to "pay" him "a little bit" for the introduction to his Chinese associates. (PSR ¶ 18).

In July 2015, the defendant met twice with the UC in Europe over the course of two days. (PSR ¶ 18).[8] During one of the meetings, the defendant stated that he knew "firsthand" that the Chinese government was actively recruiting individuals who could provide assistance, and that the Chinese government was willing to provide immigration benefits and other compensation in exchange for such assistance. (*Id.*). The UC told the defendant that he had access to classified information from a United States government agency (the "Classified Information"). (*Id.*). The defendant responded that his Chinese associates would be interested in that type of information, but that the defendant would have to travel to China to arrange a deal to provide it to them. (*Id.*).

The defendant next met with the UC after he returned to New York City in early August 2015. During the meeting, the defendant expressed concern about whether he could "hide the facts" and told the UC: "I wish that in China they didn't tell me . . . who they are . . . maybe like a handler or whatever, not 'we're with the government'" so that the defendant could simply say to his Chinese contacts "'hey, here's the stuff [*i.e.*, the Classified Information], okay, let me know what they worth' . . . ." (PSR ¶ 19). In an apparent effort to insulate himself from any potential passage of the Classified Information, the defendant told the UC: "I could get you connected and then I'm going to stay off. . . . If you make any money, just give me a little bit . . . ." (*Id.*). The defendant agreed to meet with the UC in the future in order to review the Classified Information so that the defendant could describe it to his Chinese associates, but also suggested during the meeting that the UC may be working "undercover" for law enforcement. (*Id.*). The

[8] These two meetings were not recorded. The summaries of the meetings in this submission and the PSR are based on information provided by the UC. (*See* PSR ¶ 18).

defendant later lamented: "I'm already in deep shit you know 'cause . . . people that I met you know in China over there I never disclose that, never. That's a fuckin' violation right then and there you know?" (*Id.*).

Approximately two weeks later, the UC brought a document containing the Classified Information and discussed it with the defendant in greater detail during a meeting in a hotel room. (PSR ¶ 20). The defendant examined the document and indicated that it was "definitely" classified. He said that his "people" may have difficulty understanding the Classified Information because of its subject matter, but that the Chinese military may be interested. The defendant also referred to his most recent meeting with Chinese nationals, and explained that he had been questioned regarding surveillance targets:

> I know what they want, you know, like, like, last time I spoke to them it's like, "do, do you have information on whose, who they watching, you know, in America, you know, like, like their Chinese counterpart, like the Chinese official, you know?" Who they watching, you know, that's good information to them [giggles], you know. That's good stuff for, good stuff for them, you know.

The defendant told the UC that he could not travel to China in 2015 "to meet the people," and discussed—but ultimately rejected—other options for transmitting the Classified Information such as via a third party courier or email. At the end of the meeting, the defendant declined to take possession of the classified document. (PSR ¶ 20). During a subsequent consensually recorded call, the defendant told the UC that he had caused an email to be sent to one of his Chinese associates in an effort to initiate negotiations about selling the Classified Information. (PSR ¶ 21).

During a meeting with the UC on October 22, 2015, however, the defendant indicated that he was not prepared to take further steps to transmit or sell the Classified Information at that time. (PSR ¶ 21). The defendant again indicated that he believed both he and Relative-3 were being investigated, and he said that he was concerned about having to take a

polygraph in connection with the routine background check relating to his security clearance that he expected the FBI to conduct in 2016. The defendant admitted to the UC that, during the July 2015 trip that included his meetings with the UC in Europe, one of the Chinese nationals told the defendant not to trust the UC because the UC may be part of a "set up." (*Id.*). The defendant also asked, however, that the UC maintain possession of the Classified Information until after the FBI's 2016 background check, including a polygraph that he anticipated having to take, and suggested that he would be willing to facilitate the sale once that routine investigation was completed:

Defendant:	I think, I think for now I mean **you keep this stuff** [*i.e.*, the Classified Information] you know, what you have you know. . .
UC:	Well what am I gonna do with it though?
Defendant:	Keep it, keep it, don't, don't you know. **When the time is right if I get a chance to go back**, cause um I'm thinking about going back next year you know? . . .
	* * *
Defendant:	Don't worry, don't worry. I can, I can swear, I can swear that I'm not gonna say nothing cause I'm gonna get myself in trouble too you know? Nothing like that you know, in a way. . .
UC:	Cause I'm, I didn't do anything you know like I'm, I'm, I'm legitimate businessman like. . .
Defendant:	…save the stuff you know? One day you'll, you'll understand, you know, when the time is right you know? **Just give, give me more time because I need the time**. I don't wanna deal with it cause…
UC:	Alright that, that's fine.
Defendant:	My, my, **my polygraph's coming up soon**.
UC:	Oh.
Defendant:	I, **I wanna be like, "I have a clean mind."** After that…
UC:	That's cool, that's cool, no, no, say no more. That's cool.
Defendant:	Then, then, then we can you know…
UC:	That's cool, that's cool.
Defendant:	You know what I'm saying?
	* * *
Defendant:	I wanna, in, in a way you know, I, **I know a way to beat the uh system in a way that my, my mind tends to like, like… deal with this stuff. I just forget you know?** You know? . . . [*In Chinese*: Forget, forget]. . . forgot what I did like six months ago, it just like you know?
	* * *

Defendant:	Nope, so, that's why you know I just got scared. If I, if I**, I just wanna go do my polygraph you know? The uh five-year investigation is coming up too. "Everything's clear, everything's good," ok then I still have time to play**, you know, play with. Know what I'm saying?
* * *	
Defendant:	**Yeah after everything, my, my five-year re-investigation and uh polygraph. After these done then I'm OK and free you know?** OK alright that's, and then they gonna do another five year, you know? Gotta wait another five year.

G. Post-Arrest Searches Reveal Additional Evidence

The defendant was arrested at the FBI building where he worked on March 16, 2016. He subsequently waived his *Miranda* rights and admitted to most of the foregoing activities, including to having taken steps to collect sensitive FBI information in the United States in response to taskings from Chinese Official-1. (PSR ¶ 22).

The FBI searched the defendant's New York residence pursuant to a search warrant around the time of this arrest. Agents found a .40 caliber handgun and an AR-15 rifle in the defendant's basement, neither of which was registered in New York. (PSR ¶ 23). The FBI also seized from the defendant's residence a thumb drive that contained three files with sensitive FBI information dating back to approximately 2006 and 2007. (*Id.* ¶ 24). One file—which had a "date modified" of January 19, 2007—was marked with a security header that read "FBI SENSITIVE INFORMATION FOR OFFICIAL USE ONLY." (*See id.* ¶ 24(a)). The document described technical details of FBI surveillance infrastructure, including specific information about the networks used to store data collected pursuant to the Foreign Intelligence Surveillance Act. (*Id.*). The second file contained information relating to ways in which FBI employees could access raw intelligence information, and it included network details and unique usernames for 10 FBI employees. (*Id.* ¶ 24(b)). The third file contained a spreadsheet dated June 2, 2006—with a "date

modified" of July 20, 2007—that included names and telephone numbers of FBI personnel with jobs similar to the defendant's position, as well as telephone numbers for lines that Electronics Technicians such as the defendant would have used to configure or troubleshoot network issues with the FBI's New York Office. (*Id.* ¶ 24(c)).

Also around the time of the defendant's arrest, the FBI searched a laundromat operated by members of his family and the connected upstairs apartment used by immediate relatives. The search revealed agreements with Kolion personnel and other Kolion-related documents dating back to 2005.

PROCEDURAL HISTORY

The defendant was initially charged by Complaint with four counts of making false statements, in violation of Title 18, United States Code, Section 1001, based on specific lies during the FBI's 2012 security clearance investigation and his failure to report contact with Chinese nationals on an FBI form related to his summer 2015 trip to Europe.

On August 1, 2016, the defendant waived indictment and pleaded guilty, pursuant to a plea agreement, to a one-count Information charging him with acting in the United States as an agent of China without prior notification to the Attorney General as required by law, in violation of Title 18, United States Code, Section 951(a). During the guilty plea proceeding, the defendant admitted:

> [B]etween 2011 and 2016, on various occasions I acted in the United States at the direction of an official with the Chinese government without notifying the Attorney General. My conduct included passing sensitive information to this official on several occasions. Some of my conduct occurred while I was in the Southern District of New York. At the time I knew it was wrong, and I am sorry for my actions.

(Aug. 1, 2016 Tr. 14).

THE SENTENCING GUIDELINES

The parties and the Probation Office agree that: (i) no Guideline expressly has been promulgated to apply to violations of Section 951(a); (ii) there is not a sufficiently analogous offense Guideline; and (iii) other than the Guidelines referenced in Application Note 1 to U.S.S.G. § 2X5.1, no Guidelines or policy statements can be applied meaningfully to the defendant's violation of Section 951(a). (PSR ¶ 30). Therefore, pursuant to U.S.S.G. § 2X5.1, the provisions of Title 18, United States Code, Section 3553 control. (*Id.*). In the plea agreement, the parties agreed that the appropriate Guidelines range for the Court's consideration—including credit for acceptance of responsibility pursuant to U.S.S.G. § 3E1.1—is 21 to 27 months' imprisonment, and that the applicable fine range is $10,000 to $95,000. (PSR ¶ 62). Asset forfeiture is not available for violations of Section 951.

The Probation Office recommends a sentence of 21 months' imprisonment, no fine, and one year of supervised release. (*Id.* at 20).

DISCUSSION

The Government respectfully submits that a balancing of the statutory sentencing factors set forth at Title 18, United States Code, Section 3553(a) warrants a 27-month term of imprisonment and a $95,000 fine.

A. A 27-Month Term of Imprisonment Is Appropriate

The defendant engaged in a deep betrayal of the FBI and the United States that lasted for nearly a decade by operating as an agent of the Chinese government. During that period, apparently based on little more than greed, he initially concealed that he was being groomed as a source of human intelligence through illicit relationships with Chinese nationals,[9] and later hid his

[9] "Chinese intelligence services conduct overt, covert, and clandestine intelligence collection operations against U.S. targets through a network of agents within and outside of China working

activities at the direction of Chinese Official-1. As early as January 2006, the defendant indicated that he wanted to "work together" with CC-1 and CC-2, purported managers at Kolion. Almost every year thereafter, the defendant traveled outside the United States to meet with these individuals in person so that he could convey information that he was apparently not comfortable sending via email or discussing over the phone. Consistent with that approach, and his consciousness of guilt, the defendant indicated in a January 2010 email to Relative-2 that he would ask another relative to deliver a solid state hard drive to his Chinese associates rather than sending or carrying the drive himself, and that he wanted his payment from those associates to be provided to a relative in cash that could be physically brought back to the United States so that an electronic transfer could be avoided. The defendant lied repeatedly about these relationships and activities, and was later caught on tape telling the UC about his lies. For example, he told the UC in August 2015: "I'm already in deep shit you know 'cause . . . people that I met you know in China over there I never disclose that, never. That's a fuckin' violation right then and there you know?" (PSR ¶ 19). The defendant's lengthy and intentional deception, perpetrated in travel forms, clearance-related background investigations, and at least two polygraph examinations in 2007 and 2012, is alone deserving of serious punishment.

But the most culpable aspects of the defendant's offense are his actions at the direction of Chinese Official-1, resulting in, at minimum, several confirmed disclosures of sensitive FBI information to the Chinese government. After receiving the privileges of naturalized citizenship from the United States, and a stable, well-paying job from the FBI, the defendant decided to help the Chinese government in exchange for additional compensation. He admitted

---

as—among other things—diplomats, defense attachés, and academics. They employ a variety of means to recruit and handle intelligence collectors, such as blackmail, financial incentives, and sexual entrapment." Ex. A, 2016 U.S.-China Report at 294-95.

following his arrest that he knew Kolion had ties to the Chinese government by approximately 2007, that he met Chinese Official-1 in person in 2011, and that he knew Chinese Official-1 worked for the Chinese government. The defendant told the UC that Chinese Official-1 had focused during their meetings on learning about the targets of surveillance in the United States. He then admitted to the FBI after his arrest that he disclosed sensitive information relating to FBI surveillance, technology, and organizational structure, and that he disclosed the identity of an FBI Special Agent to Chinese Official-1. By disclosing the Special Agent's identity, the defendant put the Agent and his family at greater risk of being targeted by foreign intelligence services (especially during international travel). (PSR ¶¶ 8, 14-15). And these are just the things to which the defendant admitted after being confronted by agents with specific evidence of his guilt. The Government cannot confidently assess the full scope of the intelligence breach that he caused.

As one example, the defendant did not tell the FBI during his post-arrest statement that he had sensitive FBI information in the form of three files stored on a thumb drive in his basement—in close proximity to the unregistered AR-15 that he did disclose. (PSR ¶ 24). The defendant's job did not require him to work from home, and there is no legitimate reason for him to have possessed these files at his residence. (*Id.* ¶ 25). The use of a thumb drive is consistent with the two other confirmed instances where the defendant provided sensitive FBI documents to Chinese Official-1; the defendant admitted (after being confronted) that he used similar storage media to pass an FBI organizational chart and photographs related to FBI surveillance technology to Chinese Official-1 in 2013 and 2015. (*Id.* ¶¶ 14-15). Moreover, the "date modified" on at least two of the files dates back to approximately 2007, but the defendant told the FBI that he was not acting at the direction of Chinese Official-1 until approximately 2011. Although the three files seized from the defendant's basement would have no apparent value to the type of printer-cartridge

company that Kolion purports to be, the documents would be of obvious and significant value to a foreign government. Thus, there is a great risk that the defendant provided the files that the FBI seized from his basement to Chinese nationals, placing several aspects of the FBI's digital infrastructure at risk of compromise. More importantly, these circumstances suggest that the defendant has not disclosed the full scope of his conduct and the harms that he worked on the FBI through his actions.

During the defendant's interactions with the UC, he took preliminary steps in furtherance of a plan to facilitate the sale of classified information to Chinese Official-1. He told the UC that he had sought to introduce them in Europe in July 2015, and he proposed that the UC pay him a share of any compensation that the UC received. The defendant subsequently agreed to make inquiries of his Chinese associates regarding whether they were interested in obtaining classified information from the UC, and he participated in a meeting with the UC in the United States that involved reviewing an actual classified document, which the UC told the defendant had been stolen from a SCIF. To his credit, the defendant walked away from the transaction before it was completed. But it appears that a number of factors influenced that decision, including the defendant's suspicion by at least the summer of 2015 that the FBI was investigating him, concerns about the polygraph that he expected the FBI would administer in connection with its 2016 background investigation to renew his security clearance, and warnings from his Chinese associates to be wary of the UC. In October 2015, the defendant suggested that he was simply seeking to delay the transaction, pending resolution of his routine background check, rather than abandon it. He asked the UC to retain the Classified Information so that he could have a "clean mind" and "beat the . . . system" during his upcoming polygraph, and told the UC that he would

have "time to play"—*i.e.*, help broker the sale of the classified document—after the FBI's reinvestigation of his security clearance was completed.

In addition to the intentions reflected in the defendant's communications with the UC, several other features of the case demonstrate that the defendant came all too close to committing an even more serious crime with even greater sentencing exposure than he now faces, including his access to sensitive and classified information at the FBI, his lies to the FBI for approximately a decade in order to remain in that position, and the known evidence of his actions at the direction of Chinese Official-1. *See, e.g.*, 18 U.S.C. §§ 793 (gathering, transmitting or losing defense information), 794 (gathering or delivering defense information to aid foreign government), 798 (disclosure of classified information). Indeed, based on the undisputed facts set forth in the PSR, the Probation Office initially concluded in the first draft of the PSR that an analogous offense Guideline was U.S.S.G § 2M3.3 (transmitting national defense information), and calculated an applicable Guidelines range of 37 to 46 months.

The Government agrees, as the Probation Office now does, that the appropriate range for the Court's consideration is 21 to 27 months' imprisonment, which reflects a measured approach to this prosecution that was accepted by the defendant as reasonable under the Guidelines. As stated explicitly in the plea agreement, this stipulated range accounts for the defendant's acceptance of responsibility pursuant to U.S.S.G. § 3E1.1, including a significant reduction from what the Government would otherwise have sought based on the defendant's decision to plead guilty early in the case.[10] But the defendant's conduct was both prolonged and

[10] Specifically, the stipulated range in the plea agreement accounts for the fact that the defendant waived his *Miranda* rights following his arrest and participated in an interview that spanned two days before being presented and appointed counsel, and then attempted to cooperate in a manner that was not productive. (*See* PSR ¶ 22). The defendant's attempted cooperation consisted principally of a single proffer session with the Government shortly after his presentment. The Government concluded following the meeting that he was not credible based on, among other

exceedingly serious, and specific deterrence is not a foregone conclusion in light of the fact that he is aware of highly sensitive information based on his work at the FBI that would be extremely valuable to numerous third parties. Even more important, such a sentence is needed to deter other individuals who, like the defendant, are trusted to handle sensitive information relating to the United States government or are capable of accessing it through other means,[11] which foreign powers have and will continue to go to great lengths to obtain.[12] A sentence of 27 months is therefore appropriate to achieve statutory deterrence objectives, and necessary to reflect the seriousness of the offense, to provide just punishment, and to promote respect for the law.

B. A $95,000 Fine Should Be Imposed

The Court should also impose a fine of $95,000, which is at the top of the parties' stipulated range. The Sentencing Guidelines provide that "[t]he court shall impose a fine in all cases, except where the defendant establishes that he is unable to pay and is not likely to become

---

things, shifting descriptions of his conduct relative to his post-arrest statement, and efforts to minimize and rationalize the conduct to which he admitted.

[11] "The United States will continue to face a complex foreign intelligence threat environment in 2016. We assess that the leading state intelligence threats to US interests will continue to be Russia and China, based on their capabilities, intent, and broad operational scope. . . . Penetrating and influencing the US national decisionmaking apparatus and Intelligence Community will remain primary objectives for numerous foreign intelligence entities . . . . Insiders who disclose sensitive US Government information without authorization will remain a significant threat in 2016." *Worldwide Threat Assessment of the US Intelligence Community: Hearing before the S. Armed Services Comm.*, 114th Cong. (Feb. 9, 2016) (statement of James R. Clapper, Director of National Intelligence) (emphasis added), *attached as* Exhibit B and *available at* https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf (last accessed Jan. 6, 2017).

[12] "China's infiltrations of the information systems of U.S. government organizations with a role in national security, along with infiltrations of the e-mail accounts of prominent U.S. government officials, could give China insight into U.S. government national security decision making and provide China with opportunities to manipulate it. . . . [T]hese breaches could give Chinese intelligence information useful for targeting and recruiting agents for espionage and influence operations." Ex. A, 2016 U.S.-China Report at 302-03.

able to pay any fine." U.S.S.G. § 5E1.2(a). "The burden of establishing inability to pay rests on defendant." *United States* v. *Salameh*, 261 F.3d 271, 276 (2d Cir. 2001) (citing *United States* v. *Thompson*, 227 F.3d 43, 45 (2d Cir. 2000)). Although the Probation Office concluded that the defendant does not appear to have the ability to pay a fine, the PSR reflects that the defendant has over $1.1 million in assets. (PSR at 13, 21). The estimate in the PSR is also conservative, in that it is based on a $420,000 estimate of the defendant's equity stake in his house rather than the $650,000 fair market value. (*Id.* at 13 & n.4). More importantly, the defendant reported significant liquid assets, including $264,873 in a Thrift Savings Plan, $16,878 at a federal credit union, and $2,965.11 in a Citibank Personal Wealth Management account. (*Id.* at 13). The defendant is also 47 years old, and will be able to seek to earn additional income upon completion of his sentence. *See United States* v. *Thompson*, 227 F.3d at 45 ("[A] fine may be imposed on a defendant who is presently indigent if the record contains evidence of his capacity to pay the fine from prison earnings or from earnings after his release from prison." (internal citations omitted)). Finally, the appropriateness of a fine is further supported by the unavailability of asset forfeiture in this case relating to the proceeds of the offense. *See* 18 U.S.C. 3572(a)(5) (one factor relevant to determination of a fine is "the need to deprive the defendant of illegally obtained gains from the offense"). Accordingly, the Government respectfully submits that a $95,000 fine should be imposed.

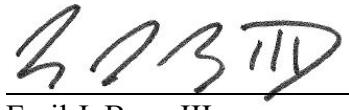
CONCLUSION

For the foregoing reasons, the Government respectfully submits that a sentence including 27 months' imprisonment and a $95,000 fine would be sufficient but not greater than necessary to comply with the purposes of sentencing.

Dated: New York, New York
January 6, 2017

Respectfully submitted,

PREET BHARARA
United States Attorney

By: 
Emil J. Bove III
Assistant United States Attorney
(212) 637-2444

Cc: Jonathan Marvinny
(Via ECF)